How to cite this article:
Amirian Farsani, A., Chelongar, E., & Aramesh, M. (2027). Challenges of Criminal Policy in Supporting Consumer Rights in the Context of Electronic Commerce. *Journal of Historical Research, Law and Policy, 5*(5), 1-12.
https://doi.org/10.61838/jhrlp.200

Article history:
Original Research

Dates:
Submission Date: 20 November 2025
Revision Date: 22 January 2026
Acceptance Date: 29 January 2026
First Pubication Date: 01 February 2026
Final Pubication Date: 01 September 2027

Challenges of Criminal Policy in Supporting Consumer Rights in the Context of Electronic Commerce

1. Amin. Amirian Farsani[1*]: Assistant Professor, Department of Law, Faculty of Humanities Sciences, University of Gonabad, Gonabad, Iran
2. Elnaz. Chelongar[2]: Department of Law, Isf.C., Islamic Azad University, Isfahan, Iran
3. Mohammadreza. Aramesh[3]: Department of Law, Isf.C.,Islamic Azad University, Isfahan, Iran

*corresponding author's email: amirian_farsani@gonabad.ac.ir

ABSTRACT

The expansion of digital interactions and the growing dependence of consumers on electronic commerce platforms have made it necessary to reconsider the traditional model of Iran's criminal policy. Despite the criminalization of certain behaviors threatening the security of online transactions in the Electronic Commerce Act and the Computer Crimes Act, the existing legislative structure remains grounded in a strict, punishment-oriented approach and fails to benefit from the leniency mechanisms provided under the Islamic Penal Code of 2013. The purpose of this study is to critically evaluate the shortcomings of the current criminal policy in consumer protection, to analyze the position of these offenses within the classification system of taʿzīr punishments, and to explain the necessity of transitioning toward a differentiated and protection-oriented criminal policy. The study employs a descriptive–analytical method through a systematic examination of Iranian legislation, relevant judicial practices, jurisprudential texts related to leniency, and comparative literature on cyber law. The findings indicate that classifying consumer-related offenses within fifth- and sixth-degree taʿzīr punishments deprives them of essential leniency mechanisms of criminal policy, such as postponement of sentencing, suspension of punishment, alternatives to imprisonment, and the institution of repentance, thereby undermining proportionality, efficiency, and justice in criminal responses. Moreover, the distinctive characteristics of electronic commerce—including relative anonymity, the involvement of third parties, and dependence on technical processes—have been overlooked, resulting in the failure to establish an effective differentiated criminal policy. The findings further show that mere criminalization and the imposition of monetary penalties paid into the state treasury are ineffective in reducing consumer vulnerability. In conclusion, the article proposes a three-tier model consisting of technical prevention, professional oversight, and consumer support and compensation as a desirable framework for criminal policy; a model that can enhance public trust, strengthen the security of electronic transactions, and contribute to reforming the existing legislative approach.

Keywords: *Criminal policy; electronic commerce; consumer rights; differentiated criminal policy; technical prevention.*

Introduction

The expansion of the digital economy in recent decades has not only transformed the traditional patterns of transactions and the seller–consumer relationship, but has also altered the nature of risks that threaten economic security and public trust. In the context of electronic commerce, the consumer operates within an environment whose fundamental characteristics include the relative anonymity of the parties, reliance on software infrastructures

and payment systems, the multilayered involvement of financial and informational intermediaries, and the high speed of data transmission. Such an environment is inherently risky and vulnerable, as it not only creates new opportunities for the commission of crimes but also increases the potential for exploitation of regulatory gaps and technical weaknesses (1).

In Iran, in response to some of these risks, the legislator has criminalized behaviors such as phishing, computer fraud, computer forgery, and unauthorized access in the Electronic Commerce Act of 2003 and the Computer Crimes Act of 2010. Nevertheless, the adopted criminal response remains predominantly punishment-oriented, strict, and grounded in the classical model of ex post reaction. Instead of focusing on intelligent risk management, technical prevention, professional regulation, and compensation for damage, this model allocates most of its capacity to the imposition of fines or imprisonment—sanctions that, in most cases, have no direct protective function for the consumer and are largely paid into the state treasury.

Moreover, the placement of these offenses within fifth- and sixth-degree taʿzīr punishments has resulted in the inapplicability of most modern institutions of criminal policy, such as postponement of sentencing, suspension of punishment, the institution of repentance, electronic monitoring, and alternatives to imprisonment. The removal of these capacities reduces both the flexibility of the criminal response and the proportionality between conduct and reaction, indicating that the legislator has not given sufficient attention to the specific nature of digital consumer crimes. At the theoretical level as well, Iran's criminal policy in the field of electronic commerce lacks a differentiated criminal policy—one that should be formed on the basis of digital governance logic and encompass three essential pillars: technical prevention, professional oversight, and compensatory–empowering support. A purely punitive approach not only fails to ensure effective prevention, but also cannot secure consumer trust solely through criminal threat, since the core of trust in the digital environment is systemic rather than personal. Accordingly, the present study seeks to demonstrate why the current framework does not meet the needs of electronic commerce and how an integrated model can address existing gaps.

The principal innovation of this research lies in its departure from a sole focus on criminalization and classical criminal liability. Instead, it reconceptualizes criminal policy within the frameworks of risk management, network governance, and restorative justice, demonstrating that a transition from punishment-centeredness to the proposed three-tier model not only provides more effective consumer protection, but also reduces the burden on the criminal justice system and contributes to trust-building in the digital market.

Concepts

Electronic Commerce

Electronic commerce refers to the conduct of all commercial activities through computer-based communication networks, particularly the Internet. This form of commerce is carried out in a paperless manner and on the basis of digital capabilities. Through electronic commerce, the exchange of purchasing and sales information, as well as information related to the transportation of goods, is conducted with minimal effort and greater speed. Companies are no longer dependent on physical limitations to establish communication with one another, and their interactions become simpler and faster.

Communication between sellers and customers can also take place on a one-to-one basis with each individual customer. In other words, electronic commerce is a general term encompassing a wide range of software

applications and systems that provide services on the Internet, such as information search, transaction management, credit assessment, credit allocation, online payment, reporting, and account management. These systems form the core infrastructure of Internet-based activities, and the objective of implementing electronic commerce is to offer innovative solutions in the field of business. This method enables merchants to continuously provide their products and services to buyers worldwide. Electronic commerce is often identified merely as buying and selling through the Internet, whereas this term reflects only a small aspect of the breadth of this domain. Today, the concept has expanded to encompass various dimensions of commerce and the economy, such that virtually any type of commercial or financial activity can now be carried out electronically (2).

Electronic commerce, as a method for electronic information exchange and the conduct of commercial transactions, has created an electronic bridge between commercial centers. Operating with a smaller volume of information—often non-uniform and commonly used among ordinary individuals—electronic commerce facilitates commercial activity (2). In its early stages, electronic commerce did not extend far beyond the informational advantages associated with commercial communication, and individuals could introduce their products through personal web pages. Statistics published from 500 companies indicate that approximately 34 percent of them used this method to advertise and promote their products in 1995, and about 80 percent did so in 1996. By the end of 2010, more than USD 220 billion in financial transactions had been conducted online through hundreds of commercial websites (3).

The Concept of Electronic Contracts

In general, electronic contracts, in terms of their essential conditions and the regulation of their legal effects, are subject to the general principles and rules of contract and obligations law. However, with regard to their technical characteristics, methods of formation, and legal protection, they require precise understanding and conformity with the general principles governing contracts. In fact, electronic contracts do not differ from ordinary contracts with respect to the validity requirements of subject matter or object; rather, they constitute a new mode of contract formation for which specific and comprehensive rules have not yet been fully developed.

The term “electronic contract” was first used in the Electronic Commerce Directive of the European Union. In the context of this directive, particularly in the section on commercial transactions, reference is made to the establishment of uniform rights for electronic contracts comparable to those of contracts concluded through paper-based and traditional instruments, without providing a concise definition of electronic contracts (4). From a legal perspective, electronic contracts are generally defined as contracts concluded through modern electronic means, such as electronic data interchange networks, electronic mail, and web pages (5).

The Concept of the Consumer

As is commonly understood, every individual in society is a consumer, and consumers—unlike other social categories such as workers or employers—do not constitute a distinct or separate class within society. In contemporary living conditions, every person necessarily meets a substantial portion of their needs for goods and services through goods and services produced and provided by others. Accordingly, the “consumer” and the act of consumption are concepts with a broad scope. First, consumption does not merely mean the purchase and use of tangible goods. A person is regarded as a consumer not only when purchasing and using goods such as a car, clothing, or food, but also when benefiting from educational services or advisory services such as legal consultation

or medical services. Second, even a grocer is regarded as a consumer when allocating foodstuffs for their own use and that of their family. Even large producers, when using the goods and services of others, are also considered consumers. Third, consumer status is not confined to a particular class or group. Affluent individuals consume just as poor individuals do; indeed, the wealthy, by virtue of greater purchasing power, may become more active consumers. In reality, it can be said that consumers encompass all people worldwide. For this reason, some equate the term “consumer” with “citizen” (6). In any event, it should not be assumed that everyone can be characterized as a consumer in all circumstances. In this regard, the fundamental question concerning the concept of the consumer is: when, and under what conditions, does a person enter the legal status of “consumer”? The answer to this question, as it appears, is not straightforward at first glance. As is well known, particular factors and necessities justify distinguishing consumers and affirming their protective entitlements. Therefore, it is necessary—through a legal approach and with due regard to all the relevant necessities and specific factors of the subject—to unpack the concept of the consumer and appropriately balance needs and necessities without sacrificing any of them. It must be acknowledged that there is no global consensus on consumer identification, and the concept remains, to some extent, ambiguous. For this reason, most domestic and international consumer-related instruments and laws provide specific definitions of the term, tailored to the objectives of each instrument. Nonetheless, in some instances these definitions are themselves ambiguous and at times overlap with one another.

Challenges of Legislative Criminal Policy in Dealing with Offenses Against Consumer Rights

Legislative criminal policy regarding offenses against consumer rights is open to criticism from two perspectives: the adoption of a “strict criminal policy,” the inability to apply the “leniency-oriented criminal policy” mechanisms of the Islamic Penal Code of 2013 to these offenses, and the neglect in adopting a “differentiated criminal policy” grounded in the principles of technical prevention, professional oversight, empowerment, consumer support, and consumer compensation (7).

Non-Applicability of Leniency Mechanisms to Offenses Against Consumer Rights

Although the Electronic Commerce Act—rather than imposing corruptive punishments such as imprisonment and flogging—has opted for the use of fines as a punitive response for various offenses against advertising regulations, which is commendable, Articles 69 and 70 of that Act determine the amount of fines for offenses against consumer rights at, respectively, ten to fifty million rials and twenty to one hundred million rials. In light of Article 19 of the Islamic Penal Code of 2013, these offenses fall within fifth- and sixth-degree taʿzīr punishments and are excluded from the scope of many provisions of the leniency-oriented criminal policy of that Code.

A notable feature of the Islamic Penal Code of 2013 with respect to minor taʿzīr offenses—particularly degrees seven and eight—is a leniency- and indulgence-oriented approach. The Code provides for exemption from punishment for perpetrators of such offenses in the event of repentance (Article 39 of the Islamic Penal Code) and stipulates that the offender’s punishment is annulled after repentance (Article 115 of the Islamic Penal Code). Likewise, a person who commits an offense of this kind will not be subject to punishment (Article 122 of the Islamic Penal Code), and these offenses are not considered effective criminal convictions (Article 25 of the Islamic Penal Code). In addition, these offenses do not entail supplementary punishments (Article 23 of the Islamic Penal Code), and the commission of a degree-eight taʿzīr offense results in the annulment of an order postponing the issuance of judgment (Article 44 of the Islamic Penal Code), an order suspending punishment (Articles 52 and 54 of the

Islamic Penal Code), and conditional release (Article 61 of the Islamic Penal Code). Moreover, postponement of sentencing is possible in respect of these offenses (Article 40 of the Islamic Penal Code). These offenses are not subject to rules on recidivism (Article 137 of the Islamic Penal Code), and it is possible to apply a semi-freedom regime (Article 57 of the Islamic Penal Code), electronic monitoring in lieu of imprisonment (Article 62 of the Islamic Penal Code), and alternatives to imprisonment (Articles 65 and 66 of the Islamic Penal Code). This policy approach in defining offenses and prescribing sanctions plays a significant role in individualizing punishments, reducing the number of convicted persons, and achieving rehabilitative objectives. However, given the level of the fines under Articles 69 and 70 of the Electronic Commerce Act and the fact that the penalties for the offenses in question are classified as degrees five and six, it is not possible to use all leniency-oriented criminal policy tools. For this reason, the legislative criminal policy in addressing the offenses under discussion is a strict and non-lenient policy (7).

Absence of a Differentiated Criminal Policy Regarding Offenses Against Consumer Rights

The nature of electronic commerce—which is fundamentally premised on the anonymity of contracting parties—cannot rely solely on bilateral trust; rather, the trust required in such transactions must be built on third-party verification or legal and technical–supervisory mechanisms. These measures provide assurance that, where the price of goods is paid before delivery, both parties—buyer and seller—can proceed with the transaction and electronic payment with confidence and reduced risk. Accordingly, adopting a criminal policy based on criminalization and punishment not only increases the cost of electronic commerce for the supplier, but also fails to provide adequate consumer protection. Therefore, a differentiated criminal policy must be adopted in this field with respect to offenses against consumer rights.

The intended differentiated criminal policy should be grounded in the three principles of technical prevention, professional oversight, and consumer empowerment and support. The preventive dimension of this policy should be based on scientific prevention and the utilization of technical methods and technological mechanisms, including the use of technical hardware and software capacities to prevent the occurrence of crime. For example, the allocation of electronic business licenses by competent institutions for the operation of online stores—similar to licensing and verifying the competence of electronic transactional enterprises—along with assigning electronic codes to goods offered in such stores, can prevent many offenses in this area. The supervisory dimension of this policy should be based on guild or professional controls and the use of self-regulatory mechanisms. In this regard, establishing a professional association of electronic sellers, adopting rules and regulations for monitoring the performance of online stores, activating systems for receiving and following up consumer complaints, and enabling professional sanctions such as warnings, blacklisting of stores, suspension, and revocation of licenses for offending stores can play an effective role in combating offenses against consumer rights. In addition, drafting professional ethics standards for electronic commerce and strengthening self-control systems play an important role in ensuring the reliability and honesty of suppliers in Internet commerce. The supportive dimension of the intended criminal policy should be based on protecting potential consumers and, where necessary, providing financial support and compensation. Enhancing consumer capacity through improving digital literacy—meaning the knowledge and skills needed to use modern communication tools—as well as increasing media literacy—meaning the ability to analyze content and understand the reality of media messages—constitutes an effective path for strengthening consumer immunity against supplier deception. Moreover, establishing a mechanism for immediate, full, electronic compensation, together with compensation for delay in payment, in the form of refunding the amount deducted from

a credit card, plays an effective role in enhancing consumer trust in electronic commerce and is superior to monetary fines that are paid into the state treasury.

Electronic payment is one of the essential and distinguishing features of electronic commerce as compared to traditional commerce. The elements involved in the electronic payment process in online purchases include the following: (a) the acquiring bank: the bank that provides the seller with special accounts titled Internet sales accounts and enables the validation and processing of the cardholder's payment; (b) the card-issuing institution: financial institutions that issue credit and debit cards (such as Visa and MasterCard) to customers and can provide required services to banks; (c) the customer: the person regarded as the cardholder; (d) the seller or merchant: the company or individual providing goods or services; and (e) third parties: systems or supervisory centers involved in the payment process among sellers, customers, and banks (8). In terms of operational flow, the electronic payment process on the Internet includes the following stages: before payment begins, the seller and buyer open bank accounts. After completing the purchase of goods or services on the merchant's website, the customer pays the purchase amount using the account number and password provided by the bank. The merchant then sends a message to the bank based on the completion of the payment operation and a request to confirm the payment. After verifying that the customer's account holds sufficient funds equivalent to the value of the purchased goods, the bank deducts the relevant amount from the customer's account and transfers it to the seller's account. Immediately thereafter, a message is sent to the merchant indicating that the payment operation has been completed and the funds have been deposited into the merchant's account (9). It should be noted that within the framework of the four principal methods of electronic payment—namely payment guaranteed by a reputable third party, payment via bank card, remote payment, and the electronic wallet—the refund mechanism via credit card and electronic wallet is applicable (9).

Offenses Threatening Electronic Commerce

Offenses threatening electronic commerce constitute part of the security challenges of electronic commerce. These offenses include phishing, money laundering, fraud, forgery, and other similar acts that jeopardize the security of electronic commerce. In what follows, this section examines these matters.

Phishing

Phishing refers to efforts to obtain sensitive information—such as passwords, user identifiers, and credit card details—by impersonating a trustworthy source. In this method, attackers, through emails or by making false promises or creating enticing offers, encourage Internet users to enter their personal information on websites created by fraudsters. This technique targets users' distrust and deception, prompting them to disclose their information in an environment that conveys a sense of security and trust, thereby causing them to be deceived by forged interfaces (10).

In another sense, phishing may be regarded as a malicious method through which, by using electronic communication tools, sensitive information such as usernames, passwords, 16-digit bank card numbers, second passwords (dynamic/OTP), and CVV2 codes are stolen. These attacks are typically carried out through social networks, auction websites, and online payment gateways and are delivered to victims via emails and messages. In phishing scams, fraudsters exploit security vulnerabilities in websites in order to conduct fraudulent operations.

This social engineering method deceives users by inducing misplaced trust in the purported security of a website. The first recorded use of the term “phishing” dates to 1987, and the term was used in 1996 to describe this method.

The techniques used in phishing take various forms. For example, tampering with and falsifying links and URLs is among the common methods. In this approach, links and addresses associated with fictitious organizations are sent by email and are, in appearance, fully similar to legitimate and original websites. The addresses may differ from the original only in minor ways, such as a one- or two-letter difference or the use of similar subdomains.

Another phishing method involves bypassing filters. In this case, phishers use images instead of text, thereby making it difficult for anti-phishing filters—primarily designed to detect text containing fraudulent addresses in emails—to function effectively.

Another example is the use of fake websites. In other words, merely entering and visiting a fraudulent site does not, by itself, complete the fraud. In some phishing methods, JavaScript commands are used to alter the address bar so that it displays a legitimate-looking URL. This is done either by placing an image of a lawful and valid Internet address in the address bar, or by closing the original address bar and opening a new address bar that contains a lawful and valid Internet address.

Computer Fraud

The term “Internet fraud” generally refers to any type of fraud in which one or more online services are used. The Federal Bureau of Investigation and police agencies across the world have appointed individuals to combat such forms of fraud. According to tables and statistics, the losses of American companies due to Internet fraud in 2003 amounted to USD 500 million (11). Computer fraud is defined in Article 13 of the Computer Crimes Act. Unlike traditional fraud, where the taking of “property” constituted the principal element of the offense, computer fraud encompasses, in addition to property, financial privileges and benefits as part of the criminalized conduct. It is also observed that, unlike traditional fraud—limited to deceiving a person—computer fraud criminalizes deception of devices and systems as well. This offense, like traditional fraud, is among result-based (material) offenses. The competent court for adjudicating this offense is the location of the bank where the account was opened. This offense is likewise among the major crimes threatening the security of electronic commerce.

Forgery

Article 523 of the taʿzīr section of the Islamic Penal Code provides: “Forgery and falsification consist of: making a writing or document, or making a seal or signature of official or non-official persons; scraping, shaving, or erasing; alteration; addition; obliteration or confirmation; blackening; advancing or delaying the date of a document in relation to the true date; attaching a writing to another writing; using another’s seal without the permission of its owner; and similar acts, with the intent to deceive.”

Unfortunately, the above provision does not define the offense of forgery; rather, it merely sets out instances of the offense, without limiting them, and concludes with the phrase “and similar acts” (12). Forgery operations may also occur through the electronic space against bank account holders—such as the forgery of electronic signatures and other manifestations—and thus constitute a threat to electronic banking. Article 6 of the Computer Crimes Act of 2010 provides: “Any person who unlawfully commits the following acts shall be considered a forger and shall be sentenced to imprisonment from one to five years, or a fine from twenty to one hundred million rials, or both: (a) altering admissible data, or fraudulently creating or inputting data; (b) altering data or signs contained in memory

cards or those processable in computer or telecommunication systems or chips, or fraudulently creating or inputting data or signs into them."

Unauthorized Access (Hacking)

Hacking refers to penetrating a computer system without the necessary authorization, ownership, or legal competence. To hack means to overcome a computer system's security arrangements in order to gain unlawful access to information stored within that system. The disclosure of passwords with the intent to access individuals' private information within an organization is among the most common computer-related violations. One of the most dangerous forms of computer delinquency involves hacking an address so that the offender can impersonate another person and carry out malicious intentions or intended crimes. A hacker is a person who gains unlawful access to computers. Such conduct may be malicious, or it may be undertaken with the intention of demonstrating the possibility of security risks. For example, Microsoft, a multinational U.S. computer technology company, and the U.S. Department of Defense are among major organizations that have been targets of hackers. Hacking is considered a risk in electronic banking systems because hackers may gain access to sensitive financial, personal, or security information, which can facilitate extortion or even—beyond that—be exploited for political or military attacks (13).

Security Challenges of Electronic Commerce

Another segment of the challenges related to protecting consumer rights in electronic commerce concerns electronic banking and bank credit cards, which will be addressed below.

The Security Coefficient of Electronic Banking

Electronic banking is a product of the growth and development of technology and has been established to facilitate banking operations. Although electronic banking offers numerous advantages and has simplified banking services for customers and the general public, it may nevertheless face security-related challenges. Account hacking, phishing, forgery of bank cards, theft of card information and data, fraud through mobile applications, and similar acts are among the most prominent examples of security breaches in electronic banking (14). From the side of banks, as well as legislative and supervisory institutions, various solutions have been proposed to improve the security coefficient of electronic banking, which overall have rendered the electronic banking environment relatively secure in terms of protecting customers' information and assets and have prevented a general erosion of public trust in electronic banking.

In any event, what is expected in terms of protecting information and assets has largely been achieved within the electronic banking system, and existing shortcomings either stem from new manifestations of security breaches—which require the development of appropriate countermeasures—or are generally attributable to the novelty of electronic banking methods. This novelty necessitates several years of implementation and operation so that weaknesses and strengths may become more evident and opportunities for remedying deficiencies may be created.

Security Weaknesses of Bank Cards in Electronic Commerce

Despite the major transformation they have brought about in electronic banking and the advantages they offer, bank cards face certain challenges from the perspective of electronic commerce security. In what follows, their vulnerabilities and weaknesses are examined in greater detail.

From the standpoint of manufacturing technology, bank cards are divided into two types, and their security threats are likewise concentrated around these two principal types. In magnetic stripe cards, customer information—such as the card number, verification code, and expiration date—is stored on the magnetic stripe on the back of the card. This information is converted into unique data symbols that are then translated into numbers for user comprehension and use in electronic gateways. Since these symbols function as usage criteria and are not measurable, the application of mathematical operations to them is not possible. This type of card is known as a "processable card." When the card is inserted into a device, its information is transmitted to the bank's centralized systems, and if verified, the customer may use the card instantaneously or online.

For this reason, preventing unauthorized access through physical terminals requires both possession of the card and entry of a password. In other words, offenders must either use the user's original card or copy the card's symbols onto another blank card. Such copying does not correspond to any of the material acts of forgery, since altering or inputting data implies modification of existing data, while creating data implies bringing into existence data that did not previously exist. Moreover, unauthorized access is likewise inapplicable here, because magnetic cards issued by banks lack sufficient protective measures; therefore, committing this act is classified as theft (15).

Another common method for stealing bank card information involves the use of skimmer devices. These devices can be installed on point-of-sale terminals and automated teller machines. Users of modern banking systems who are unaware of the installation of such devices effectively disclose their card's security information. This method places computer theft within the category of deceptive and fraudulent crimes. Accordingly, the criminal strategy for addressing computer theft in the field of modern banking should emphasize reform and rehabilitation. Such an approach is necessary because the dangerousness indicators associated with this offense—in terms of criminal propensity and social maladjustment—are very high, and the offender requires rehabilitation. It appears that achieving this objective is feasible in dealing with computer thieves. For example, one computer offender who was released from prison after eight months stated that he had learned from his past mistakes and would never again produce malware, emphasizing that he would not expose security vulnerabilities or allow computer systems to proliferate at the network level (15).

The second type of bank card is the smart card. In this card, instead of a magnetic stripe, a microprocessor is embedded, and electronic money—as a form of independent financial data—is stored within the microprocessor. For this reason, it is also known as an electronic wallet. Although in most cases chips do not possess the physical identity of a card, by virtue of their processing capability and memory, such cards are regarded as a type of chip.

In practice, a smart card functions like a small computer that, without needing to connect to the bank's central servers, communicates offline with the banking terminal. If the card's microprocessor is not satisfied with the validity of access, it will not permit the card reader to withdraw or transfer funds. Smart cards are, from a technical standpoint, computer systems. If the card's memory is manipulated or altered, the crime of card forgery is realized—even if the manipulation is carried out by the cardholder—because the bank is the creator of the data stored on the card, and the cardholder merely possesses the data.

Accordingly, if the cardholder increases the balance by manipulating the memory—since such conduct contradicts the bank contract—this act is deemed unauthorized. Similarly, if the cardholder creates obstacles such that information related to settlement of their debt is not processed through banking gateways, while data editing prevents a reduction in the card's stored balance, this conduct—because it alters the functionality and performance of the card's microprocessor through data manipulation—constitutes the offense of disrupting a computer system (16). In crimes arising from security weaknesses of bank cards, it makes no difference whether the act is committed using a valid card or a card that has been deactivated and whose number has been invalidated. In any case, such actions cause non-material harm to the bank, damage its commercial reputation and credibility, and result in the loss of customers. The final stage of unauthorized access involves the use of a forged card; if a bank card is forged by an individual and used to conduct banking operations at physical terminals, this circumstance gives rise to a plurality of material offenses.

Conclusion

The present study demonstrated that Iran's criminal policy in addressing offenses against consumer rights in the context of electronic commerce has not yet aligned itself with the logic of data-driven governance and the security requirements of the digital economy. The existing framework of criminalization is largely centered on ex post criminal responses and the imposition of fines and imprisonment, whereas the nature of offenses occurring in electronic environments requires, more than severity, precision, speed, technical prevention, and trust-enhancing mechanisms. Classifying a significant portion of these offenses within fifth- and sixth-degree taʿzīr punishments has rendered many modern capacities of the Islamic Penal Code—such as postponement, suspension, semi-freedom regimes, electronic monitoring, leniency institutions, and even mechanisms for avoiding recidivism—practically inapplicable. The result is a strict yet low-yield response that neither produces effective deterrence, nor ensures full compensation for consumer harm, nor contributes to the formation of sustainable trust in electronic commerce. Examination of the theoretical structures further showed that electronic commerce is founded on multilayered, data-based systems in which the roles of contracting parties, payment intermediaries, financial system operators, electronic gateways, and supervisory bodies all interact with one another. Such a structure requires a criminal policy that attends not only to criminal conduct, but also to the environments that generate the possibility of crime. Neglecting this reality has reduced the issue to "crime" alone and overlooked "crime-generating mechanisms," thereby intensifying the inefficiency of criminal responses. Ultimately, transitioning from the current situation necessitates the development of a differentiated criminal policy—one designed on the basis of the technical, economic, and legal characteristics of electronic commerce and capable of establishing a balance between necessary criminalization, effective prevention, and immediate compensation. The three-tier model proposed in this study—namely the integration of technical prevention based on standardization and data authentication, professional oversight and self-regulation, and restorative consumer protection accompanied by rapid and accurate compensation—can substantially address existing gaps. Implementing such a model would reduce pressure on the judicial system, enhance the security and predictability of digital transactions, and create conditions in which consumers, instead of remaining potential victims, become active, informed, and empowered participants in the digital economy. This transformation represents the starting point for the evolution of Iran's criminal policy in confronting the realities of the data-driven era and can lay the groundwork for an indigenous model of criminal governance in electronic environments.

Acknowledgments

We would like to express our appreciation and gratitude to all those who helped us carrying out this study.

Authors' Contributions

All authors equally contributed to this study.

Declaration of Interest

The authors of this article declared no conflict of interest.

Ethical Considerations

All ethical principles were adhered in conducting and writing this article.

Transparency of Data

In accordance with the principles of transparency and open research, we declare that all data and materials used in this study are available upon request.

Funding

This research was carried out independently with personal funding and without the financial support of any governmental or private institution or organization.

References

1. Ebrahimpour A, Ghandour M. Foundations of E-Commerce. Tehran: Sahel-e-Zendegi Publishing; 2018.
2. Mirzaei H. Electronic Commerce. Tehran: Shaparak-e-Sorkh; 2020.
3. Jafari Tabar M. Electronic Commerce. Tehran1996.
4. European Union. Council Directive 87/102/EEC of 22 December 1986 on the approximation of the laws, regulations and administrative provisions of the Member States concerning consumer credit. Official Journal. 1986(L42).
5. Maghami-Nia M. The method of concluding electronic contracts and their characteristics. Civil Law Knowledge. 2012(1).
6. Hosseini M, Ghaffari Farsani B. How to apply competition law rules to the internet domain market. Legal Journal of New Technologies. 2021(1).
7. Heidari AM. Crimes against advertising rules in e-commerce. Criminal Law Research. 2014(1).
8. Fathian M, Molanapour R. Electronic Commerce. Tehran: Ati-Negar; 2011.
9. Nedal SB. Rules of E-Commerce Contracts. Amman: Dar al-Thaqafa for Publishing and Distribution; 2009.
10. Razavi M. Cybercrimes and the role of the police in preventing and detecting these crimes. Entezam-e-Danesh Quarterly. 2007(32).
11. Khorramabadi A. Computer fraud from an international perspective and the situation in Iran. Law Quarterly, University of Tehran. 2007;37(2).
12. Mir-Mohammad-Sadeghi H. Crimes Against Public Security and Peace. Tehran: Mizan; 2015.
13. Ahmad-Al-Hashem M. Cybercrimes and the role of the police in preventing and detecting these crimes. Entezam-e-Danesh Quarterly. 2010(32).

14. Qarani D. A review of electronic banking in Iran: The necessity of its development and security. Journal of Management, Financial and Accounting Economics Studies. 2017(2).

15. Mir-Mohammad-Sadeghi H, Azari Matin A. Criminal strategies in modern banking with emphasis on electronic signatures. Rahbord Journal. 2017(82).

16. Gerayeli MB. An investigation into computer forgery, destruction, and disruption. Criminal Law Doctrines. 2010(14).